Department of Homeland Security Daily Open Source Infrastructure Report for 10 February 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Memphis Business Journal reports First Tennessee Bank has reported the circulation of counterfeit cashier's checks bearing the institution's name and routing number, according to a statement released by the Federal Deposit Insurance Corp. (See item 9)
- The investigation into the December 8 crash of a Southwest Airlines 737 at Midway International Airport has revealed a lack of federal requirements for calculations critical to landing planes in wintry weather; the Federal Aviation Administration has begun an evaluation of landing standards. (See item 11)
- The Cleveland Plain Dealer reports the number of Ohioans dying from the antibiotic−resistant strain of intestinal bacteria Clostridium difficile jumped 20 percent between 2000 and 2005, when the aggressive infection contributed to an estimated 785 deaths. (See item 26)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 08, Computerworld* — **Power grid in Houston to get smart technology upgrade.** A Houston−based electric and gas utility company is using new technology to make its power grid more efficient by enabling it to automatically report power outages and component failures over

a real−time, IP−based broadband−over−power−line (BPL) system. CenterPoint Energy Houston Electric LLC is deploying a pilot of an “intelligent grid” that will allow the power grid to transmit its status using strategically placed sensors and new “smart” electric meters planned for installation in all customer homes and businesses. Under the pilot project, several hundred sensors will be placed in strategic locations throughout the power grid and connected to a pilot BPL system. The sensors will be like eyes and ears that can deliver information on the condition of the system, including voltages and other feedback, via the BPL system directly to databases and analytical software. The program will be deployed in three areas in Houston this year, covering 44,500 electrical customers and 22,500 natural gas customers.
Source: http://www.computerworld.com/printthis/2006/0,4814,108493,00 .html

2. *February 08, North American Electric Reliability Council* — **North American Electric Reliability Council adopts 16 reliability standards.** The North American Electric Reliability Council (NERC) approved 13 new reliability standards and approved revisions to three existing standards on Tuesday, February 7. The standards cover seven critical reliability areas: vegetation management, facility ratings, transfer capabilities, reliability coordination, verification of generator capabilities, transmission and generation protection systems, and undervoltage load shedding. “...We have adopted 16 new or revised reliability standards that will promote greater reliability and conformance throughout the industry in key reliability areas,” said Rick Sergel, NERC president and CEO. A new standard on vegetation management will reduce transmission outages caused by vegetation near transmission rights−of−way. Two new standards on facility ratings set the minimum criteria in the calculation of facility ratings to plan and operate the bulk electric system. Two new standards require that transfer capabilities are documented and communicated to constituents. Three new standards expand the operating and situational awareness requirements for reliability coordinators. Revisions to three existing standards specify regional reliability organization procedures for analyzing and reporting generator relay misoperations. The revised standards also add requirements for generator owners to report relay misoperations and to have a documented program for relay maintenance.
For further information:
ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/02−08−06_Standards−PR.pdf
Source: https://standards.nerc.net/

3. *February 08, Associated Press* — **Alaska pipeline may be easy terrorist target, but looks can be deceiving.** The trans−Alaska pipeline looks like it would be an easy target for terrorists intent on destroying a valuable American asset, but those responsible for its safekeeping say looks can be deceiving. The 800−mile pipeline −− which carries nearly 17 percent of domestic crude oil production −− snakes north to south across Alaska. About half of the 48−inch diameter pipeline lies underground. The other half is visible. Terrorism experts say pipelines in general are easy targets, but tend to be low priority because they can be repaired so quickly. And officials with an intimate knowledge of the pipeline say it's far less vulnerable than it appears −− in part because of the difficulty a saboteur would have getting any weapon capable of serious damage into Alaska. The pipeline has state, federal, and local agencies keeping an eye on it, said John Madden, deputy director of the state Division of Homeland Security and Emergency Management. Agencies including customs, immigration, border control and state troopers, work to make sure that such a weapon would never make it into Alaska, he said. “There are quite a bit of those layers of defense and observation which the public will never see,” Madden said.

Source: http://www.coloradodaily.com/articles/2006/02/09/news/beyond_boulder/news6.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *February 09, Alice Echo−News Journal (TX)* — **Diesel spill shut down Texas highway.** An early morning accident just outside Alice, TX, shut down part of Highway 281 for several hours Tuesday, February 7, while crews worked to clear a hazardous material spill, Department of Public Safety (DPS) officials said. A box truck containing produce was traveling southbound on Highway 281, when the driver reportedly lost control of the vehicle and exited the roadway. DPS officials said the truck re−entered the lane, but the driver over−corrected to the left, causing the cargo in the rear of the vehicle to shift. The shifting cargo threw the vehicle over onto its right side, and the truck reportedly skidded 250 feet on the roadway before coming to a stop shortly before 6 a.m. CST. No other vehicles were involved in the accident. A hazardous materials team from Alice was called to the scene to help contain a diesel fuel leak that occurred as a result of the accident, but that material was cleared.
Source: http://aliceechonews.com/articles/2006/02/08/local_news/news 04.txt

5. *February 08, KOTV (OK)* — **Gasoline tanker truck accident causes leak, shuts down intersection in Oklahoma.** A traffic accident caused a potentially dangerous situation at a Tulsa, OK, intersection Wednesday afternoon, February 8. As a tanker truck approached the intersection of 21st and Southwest Boulevard, the tank slammed into the cab of the truck causing a portion of the tank to rupture and leak gasoline. Firefighters shut down the intersection until the leak was plugged. No one was injured.
Source: http://www.kotv.com/main/home/stories.asp?whichpage=1&id=985 10

[Return to top]

Defense Industrial Base Sector

6. *February 09, Defense News* — **QDR seeks capabilities, not weapons.** The Pentagon's acquisition of intelligence, sensors and reconnaissance equipment will be the first to undergo an experiment aimed at determining how to buy broad capabilities instead of specific weapons for individual military services. The just completed Quadrennial Defense Review (QDR) recommends that the Pentagon budget be structured according to "joint capability" areas instead of dividing by military departments. The change would require that monies be allocated likewise. Stephen Cambone, the U.S. undersecretary of defense for intelligence is "doing a prototyping of the intelligence, sensors and reconnaissance capabilities" to determine how to buy them on a joint basis, said Ryan Henry, the principal deputy undersecretary of defense for policy and one of the key architects of the QDR. "How that will be implemented is a work−in−progress." During the next few months, joint logistics and joint command−and−control areas will undergo similar "prototyping," Henry said Wednesday, February 8. Kenneth Krieg, the U.S. undersecretary of defense for acquisitions, will examine ways to alter the Pentagon's buying process to determine how systems that are currently bought with a specific military service in mind can be altered to fit the joint capabilities approach

recommended by the QDR, Henry said.
Source: http://www.defensenews.com/story.php?F=1524029&C=america

[Return to top]

Banking and Finance Sector

7. *February 09, Reuters* — **Britons face chip−and−pin future in fraud fight.** From next week, a signature will not be good enough to buy goods or services across Britain. The deadline for shoppers to remember their debit and credit card pin numbers is Tuesday, February 14. From then on, cardholders are no longer assured the option of signing to verify a purchase and may have their cards refused. Banks and retailers have introduced chip−and−pin technology in recent years to halt rising card fraud, requiring an increasing number of shoppers to enter their four−digit PIN numbers to verify card purchases. British payments association APACS estimated that 127 million chip−and−pin−enabled cards have been issued since 2003, out of about 140 million cards in circulation. APACS said that, if left unchecked, the level of fraud on UK debit and credit cards could have topped $1.4 billion annually, up from 2004, but the use of chip and pin should stem that rise. But some retailers are not ready for the technology. They can choose to accept signatures but will take on responsibility for making good on losses from fraud. APACS estimated more than 80 percent of tills in the UK were upgraded to accept chip−and−pin cards by the end of 2005.
Source: http://wireservice.wired.com/wired/story.asp?section=Technol ogy&storyId=1156643

8. *February 08, SecureIDNews* — **Banks compare cost, quality, and strength of multi−factor authentication schemes.** Federal guidance has recommended that financial institutions (FI) boost the strength and security of their online banking systems by the end of 2006. Recent guidelines by the Federal Financial Institutions Examination Council (FFIEC) suggest a range of options. In the FFIEC report, “Authentication in an Internet Banking Environment,” FIs are urged not only to assess their risks of fraud, but to consider strong−authentication methods such as one−time password generators, PKI−based systems, and smart cards. How well a bank prevents fraudulent activity with its authentication system depends on the success of three factors commonly used to authenticate: the knowledge factor (something you know, like a password); the possession factor (something you have − such as a token); the self factor (something you are − such as a fingerprint). Strong authentication generally combines factors together (e.g. a possession factor plus a knowledge factor) and thus can be considered multi−factor authentication. In 2006, huge strides are being made to create open frameworks for strong authentication, and so a greater range of products will be interoperable. The Initiative for Open Authentication and the Liberty Alliance have already produced open specifications they hope to expand.
Source: http://www.secureidnews.com/library/2006/02/08/banks−compare −cost−quality−and−strength−of−multifactor−authentication−sch emes/

9. *February 08, Memphis Business Journal* — **First Tennessee reports counterfeit cashier's checks.** First Tennessee Bank has reported the circulation of counterfeit cashier's checks bearing the institution's name and routing number, according to a statement released Wednesday, February 8 by the Federal Deposit Insurance Corp. The counterfeit checks are identifiable by a number of features, including that they have been printed on standard green

check stock with a dark green border and gold seal in the middle, unlike the authentic checks, which are light blue with a white stripe and star. They have the name of the institution placed beneath its logo, rather than to the right as on authentic checks. And authentic checks do not have an actual signature line. All falsified checks to date have been made in the amount $3,975 and have the date of either Saturday, January 7, 2006 or Sunday, January 8, 2006, show the remitter as Agnes Lawsonn and indicate they were issued from center No. 7274. A spokesperson for First Tennessee declined to comment on how many have been found or at which locations.
Source: http://www.bizjournals.com/memphis/stories/2006/02/06/daily2 8.html?from_rss=1

10. *February 03, Congressional Research Service* — **Report: Data Security: Federal and State Laws.** Security breaches involving electronic personal data have come to light largely as a result of the California Security Breach Notification Act, a California notification law that went into effect in 2003. In response, the states and some Members have introduced bills that would require companies to notify persons affected by such security breaches. By December 2005, 35 states had introduced data security legislation and 22 states had enacted data security laws. Numerous data security bills have been introduced in the 109th Congress and several were reported by Senate committees. This report provides a brief discussion of federal and state data security laws.
Report: http://www.opencrs.com/rpts/RS22374_20060203.pdf
Source: http://www.opencrs.com/document/RS22374

[Return to top]

Transportation and Border Security Sector

11. *February 09, USA TODAY* — **Airlines' landing rules get additional scrutiny.** The investigation into the December 8 crash of a Southwest Airlines 737, Flight 1248 at Chicago's Midway International Airport has revealed a lack of federal requirements for calculations critical to landing planes in wintry weather. The Federal Aviation Administration has begun an evaluation of landing standards, said spokesperson Laura Brown. Not all airlines would have allowed a landing on the night of the Chicago crash. Continental Airlines' pilot manuals for its fleet of 737−700s show that Midway's runway was hundreds of feet too short for a landing in the conditions that existed December 8. That two large airlines could reach such different conclusions about whether to land "is certainly a question that is significant," said Kevin Darcy, a safety consultant who formerly headed Boeing's accident investigation division. Slowing a jet speeding at more than 100 mph requires complex equipment and skillful piloting, especially when snow, slush or ice cover a runway. Many factors −− such as a plane's weight and the wind direction −− can dramatically change how far it takes to stop. European aviation regulations have tighter standards on landing calculations; they require that carriers add a 15 percent safety margin when computing the landing distance in flight.
Source: http://www.usatoday.com/travel/flights/2006−02−08−airlines−l anding−rules_x.htm

12. *February 09, USA TODAY* — **Chicago's congested skies spur difficult discussions.** Debate about Chicago's airports has intensified since a Southwest Airlines jet skidded off a runway at Midway International Airport nine weeks ago, renewing questions about congestion and expansion. There also are questions about the future of O'Hare International Airport. Court

challenges could delay a long−planned $6.6 billion expansion at O'Hare, which has been overtaken by Atlanta's Hartsfield−Jackson as the world's busiest airport. Last week, the Department of Transportation said the two city−owned airports ranked last among 33 big U.S. airports for on−time departures in December. At O'Hare, 60 percent of flights left on time; 65 percent were on time at Midway. And, for decades, there has been talk about developing a new airport near Peotone in suburban Will County to take pressure off O'Hare and Midway. Discussions about an airport south of Chicago began in the 1960s. The state allocated $75 million for land acquisition near Peotone beginning in 2002. But two members of Congress disagree over the proposed airport. Adding to the uncertainty, the Gary−Chicago International Airport in Indiana got $57.8 million in federal funds last month for an expansion its boosters say will make it the region's third major airport.
Source: http://www.usatoday.com/travel/flights/2006−02−08−chicago−co ngested−skies_x.htm

13. *February 09, Associated Press* — **Jet lands in Denver after apparent suicide.** A man apparently hanged himself in an airplane lavatory during a flight that was diverted to Denver after his body was discovered, police said. Denver medical examiner's spokesperson Michelle Weiss−Samaras said an autopsy was planned for the body of Gerald Georgettis, 56, of Miami, which was found Wednesday, February 8, on a United Airlines flight from Washington, DC, to Los Angeles.
Source: http://www.usatoday.com/news/nation/2006−02−09−denver−jet_x. htm

14. *February 09, Bangor Daily News (ME)* — **Lost men carrying explosives enter U.S.** On Tuesday, February 7, two Canadian construction workers crossed the border carrying a load of explosives without stopping at the border crossing. They were apprehended, but were later released and returned to Canada. Sometime Tuesday morning the two unnamed Canadians were supposed to deliver a load of explosives to a construction project on the Trans Canada Highway in northwest New Brunswick. Spokesperson Brian Lundquist said the two men, who were looking for the remote site to deliver the explosives got lost and somehow ended up at the border crossing. They reportedly didn't know where they were, and failed to stop at the U.S. Custom and Border Protection station at Fort Fairfield, ME. The Border Patrol was alerted. Lundquist said the pair was tracked down and arrested. After an investigation, the explosives were delivered to the construction project. And, Lundquist said there will be no federal charges. "It was an innocent mistake," Lundquist said, "The men and the explosives have been returned to Canada."
Source: http://www.bangornews.com/news/templates/?a=128748

15. *February 09, Government Accountability Office* — **GAO−06−374T: Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program (Testimony).** After the events of September 11, 2001, Congress created the Transportation Security Administration (TSA) and directed it to assume the function of passenger prescreening −− or the matching of passenger information against terrorist watch lists to identify persons who should undergo additional security scrutiny −− for domestic flights, which is currently performed by the air carriers. To do so, TSA is developing Secure Flight. This testimony covers TSA’s progress and challenges in (1) developing, managing, and overseeing Secure Flight; (2) coordinating with key stakeholders critical to program operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing impacts on passenger privacy and protecting

passenger rights. This testimony includes information on areas of congressional interest that GAO has previously reported on. In a prior report, the Government Accountability Office (GAO) recommended that the Department of Homeland Security (DHS) direct TSA to take several actions to manage risks associated with Secure Flight's development, including finalizing system requirements and test plans, privacy and redress requirements, and program cost estimates; and establishing plans to obtain data needed to operate the system. DHS generally concurred with GAO's recommendations, but has not yet completed the actions it plans to take.
Highlights: http://www.gao.gov/highlights/d06374thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−374T

[Return to top]

Postal and Shipping Sector

16. *February 09, Associated Press* — **San Francisco postal worker held on alleged rampage threat.** A former postal worker was arrested on federal charges after he allegedly threatened to kill his one−time colleagues, postal authorities said. Michael Anthony Kennelly, 52, is accused of calling a U.S. Postal Service processing and distribution center in San Francisco last week and vowing to duplicate a suicidal rampage involving another former postal worker two days earlier in Santa Barbara County that killed eight people, postal authorities said Monday, February 6. Kennelly faces charges of threatening a federal official. Kennelly was fired from the distribution center in 2002 for chronic absenteeism and had a history of calling the post office drunk and "ranting and raving," said U.S. Postal Inspector Marius Greenspan. Kennelly admitted to making the telephone call but denied making threats against postal employees, Greenspan said. The affidavit said Kennelly had arrests dating to 1975 for carrying a concealed weapon, obstructing police, sexual battery, and drunken driving.
Source: http://cbs5.com/topstories/local_story_038210333.html

17. *February 08, Daily Home Online (AL)* — **Post Office evacuated after suspicious package found.** A suspicious package at the Pell City, AL, U.S. post office on Tuesday morning, February 7, prompted an evacuation of the building and a bomb squad investigation. During the investigation, Jefferson County Bomb Squad personnel determined the package was not dangerous and the post office was reopened. The incident began at 8:06 a.m. CST when postal employees called Pell City police to report a suspicious package had been left unattended overnight on a counter in the public access area, Pell City Police Lt. Don Newton said. The package had not been there when postal employees left work Monday night. Newton said police and fire personnel arrived at the scene, evacuated the building and set up a perimeter blocking access to the parking lot. Once the scene was secured, authorities waited for Jefferson County Bomb Squad Lt. Byron Jackson and Deputy Kerry Morgan to arrive at the scene to investigate the package. "It contained bottles of perfume," Jackson said. Newton said that while the package did not contain a dangerous substance, the use of precaution was warranted. Newton said, "I would rather expend the resources and play it safe than take a chance."
Source: http://www.dailyhome.com/news/2006/dh−pellcity−0208−dthompso n−6b07v2200.htm

[Return to top]

Agriculture Sector

18. *February 09, Agricultural Research Service* — **Cacao symposium tackles chocolate production problems.** Agricultural Research Service (ARS) scientists have located genetic markers for resistance to a major disease of cacao trees, the source of seeds for cocoa and chocolate. The scientists found the markers for resistance to witches' broom, a disease caused by the fungus Moniliophthora perniciosa, the main killer of Theobroma cacao trees. They are presenting this and other research findings during a biennial Symposium on Cocoa hosted by the National Academy of Sciences on February 9−10 in Washington, DC. Witches' broom penetrates cacao stem and fruit tissue, inhibits formation of seedpods and destroys mature pods. Two other major cacao−production problems being addressed by ARS researchers are frosty pod and black pod rot. The symposium, titled "Theobroma cacao: The Tree of Change," features presentations on cocoa−related aspects of plant and biomedical science, sustainable agriculture, nutrition, medicine and anthropology, along with round−table discussions on problems and issues facing cocoa−growing regions of West Africa, East Asia and the Americas.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

19. *February 09, WBBH (FL)* — **Crop disease threatens tomatoes.** A highly−contagious disease has been found on a crop of tomato plants in Immokalee, FL. Late blight can destroy tomato crops in just days. An alert was sent out to all Southwest Florida farmers to take precautions, because the disease spreads easily and quickly. At Oakes Farmers Market in Naples, FL, they're already feeling a Wilma−induced tomato shortage. If late blight spreads, researchers believe our only options will be international. "We're going to be going to other sources, like Mexico and Honduras," said Lee Snyder of Oakes Farmers Market. A team of University of Florida researchers, is testing different fungicides to see which one stops late blight before it has time to spread.
Late blight information: http://ohioline.osu.edu/hyg−fact/3000/3102.html
Source: http://www.msnbc.msn.com/id/10841254/

20. *February 09, Agence France−Presse* — **Japan to kill 45 cows for fear of mad cow disease.** Japan said it will kill 45 cows at a farm for fear of mad cow disease. Japan ordered the killing after the death of a Holstein that in its infancy was fed meat−and−bone meal, which is no longer used in Japan and other countries because it is believed to pass on the brain−wasting disease. The cow died on January 20 at the farm on the northern island of Hokkaido at the age of five years and four months. It was confirmed three days later to be Japan's 22nd case of mad cow disease or bovine spongiform encephalopathy (BSE). The Hokkaido prefectural administration said in a statement the milk cow was fed meat−and−bone meal before the feed was banned in Japan in September 2001 when the country's first BSE case was discovered. It was the first time a cow fed with meat−and−bone meal was found to be infected with BSE in Japan, the only Asian country to have confirmed cases of the disease. Japan will incinerate 43 other female Holsteins, which lived close to the infected cow or fed on the same meat−and−bone meal at the farm, as well as two calves borne to it after testing them for mad cow disease.
Source: http://news.yahoo.com/s/afp/20060209/hl_afp/japanustradehealth_060209093409;_ylt=Al8NorlYuF96jnWMB8BpSkyJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

21. *February 09, Calgary Sun (Canada)* — **Cull of wild deer targets disease.** More than 500 wild deer are to be shot and tested during the next month in Canada, as efforts are stepped up to curb the spread of chronic wasting disease (CWD). The cull of 250 animals each in the South Saskatchewan and Red Deer river valleys −− and a yet−to−be−decided number at a provincial park near Lloydminster −− will determine if there are any new cases since four infected animals were found late last year in Alberta, said Lyle Fullerton, a spokesperson for Alberta Fish and Wildlife. "It's part of what we're calling enhanced surveillance to find out if CWD has spread upstream from these positive cases," Fullerton said, adding the Alberta infections were the first found there since the province started monitoring for CWD in 1996. "We certainly hope there are no new ones in Alberta, but there are some new cases of CWD immediately east of the Alberta−Saskatchewan border."
CWD information: http://www.cwd−info.org/
Source: http://calsun.canoe.ca/News/Alberta/2006/02/09/1432823−sun.h tml

22. *February 08, BBC News* — **Foot−and−mouth cases in Argentina.** Authorities in Argentina have reported an outbreak of foot−and−mouth disease (FMD) near the border with Paraguay. The National Service for Food Safety and Quality said it had found some 70 cattle showing signs of the infection in the province of Corrientes. Argentina, one of the world's leading beef exporters, was hit by a FMD crisis five years ago. A senior health official said the latest outbreak was isolated and that its origin was still unclear. The head of the National Service for Food Safety and Quality, Jorge Amaya, warned that some 3,000 cattle in the area may have been infected. Officials sealed off an eight square mile area to contain the disease. FMD is a highly contagious illness that affects cows, sheep, pigs and goats. Argentina has had fewer problems with FMD than other countries in Latin America −− there have been recent outbreaks in neighboring Brazil and Paraguay.
FMD information: http://www.vet.uga.edu/vpp/gray_book/FAD/FMD.htm
Source: http://news.bbc.co.uk/2/hi/americas/4694532.stm

[Return to top]

Food Sector

23. *February 09, Associated Press* — **Japan's ruling party sending inspection team to U.S. beef facilities.** Japan's ruling party said Thursday, February 9, it would sending inspectors to U.S. beef facilities amid Tokyo's ban on American meat. Japan halted U.S. beef imports last month after the discovery of backbones in a shipment of American veal. The bones are deemed to be at risk of mad cow disease and are banned under a deal that reopened the Japanese market to beef in December. The Liberal Democratic Party delegation will leave Thursday, February 9, on a trip that will include a stop at a Tyson Foods Inc. facility in Kansas, according to an itinerary the party provided. A recent fact−finding mission sent by opposition lawmakers reportedly found the Kansas facility did not completely remove banned parts from the beef it processed. Tyson Foods has protested the claim. Also Thursday, a senior agricultural official said reports that downer cattle were used for meat in the U.S. may further delay a resumption of American beef imports. The U.S. Department of Agriculture has found that meat from 20 downer cattle −− animals who have difficulty walking −− were released into the market, vice farm minister Mamoru Ishihara said at a press conference.
Source: http://www.kansas.com/mld/kansas/13824492.htm

24. *February 08, Agence France−Presse* — **Netherlands to cull 3,500 pigs in dioxin scare.** Dutch health authorities were to begin carrying out a preventative cull of some 3,500 pigs from 10 farms that bought animal feed which could contain high concentrations of cancer−causing dioxin. "The farmers together with the food safety authorities have decided on the preventative measure of culling all pigs of over 110 pounds from some 10 farms that bought large quantities of this animal feed," the Dutch food safety watchdog VWA said. Illegally high dioxin levels were identified in January in pork fat bought in Belgium by a Dutch animal feed company. The authorities quarantined 275 farms to prevent high levels of dioxin −− a powerful carcinogen −− from entering the food chain. A total of 144 farms remain under quarantine in The Netherlands because of the dioxin scare.
Source: http://news.yahoo.com/s/afp/20060208/hl_afp/netherlandshealth_060208172613;_ylt=Aoi.Mzopi9cL151FGl6ZMd6JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Water Sector

25. *February 08, Waste News* — **Township ordered to fix sewer system after spills.** Pennsylvania is ordering Paint Township to do something about its malfunctioning sewer system, which has spilled untreated sewage into a Clarion River tributary for several years. The state Department of Environmental Protection (DEP) sent the township a notice of violation in December 2003 because it failed to implement an action plan to install additional sewer lines. Paint Township did not respond to the notice in a way that would address the sewer problems, which consist of malfunctioning on−lot systems, DEP said.
Source: http://www.wastenews.com/headlines2.html?id=1139422190

[Return to top]

Public Health Sector

26. *February 09, Cleveland Plain Dealer (OH)* — **Ohio deaths from Clostridium difficile bacteria rise rapidly.** The number of Ohioans dying from the intestinal bacteria Clostridium difficile (C. diff) jumped fourfold between 2000 and 2005, when the aggressive infection contributed to an estimated 785 deaths, Ohio Department of Health (ODH) records show. New data shows C. diff infections rank among the deadliest infectious diseases in the state, and the toll may be greatest in the Cleveland area. Data for 2005 is incomplete, but nearly one−third of the confirmed victims lived in the seven−county area. ODH began examining death certificates in January. Deaths where C. diff was a main underlying cause quadrupled statewide, but the agency also found the numbers jumped substantially higher when C. diff was recorded as a contributing cause. By that measure, C. diff−related deaths jumped 20 percent between 2004 and 2005 estimates. A superstrain of C. diff has been blamed for scores of deaths in Canada and Britain. The antibiotic−resistant strain has been confirmed in more than a dozen states, including Ohio. But no other state has compiled data to determine the toll, said Dale Gerding, a C. diff expert at Loyola University.

Clostridium Difficile information: http://www.cdc.gov/ncidod/dhqp/id_Cdiff.html
Source: http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/113947813986740.xml&coll=2

27. *February 09, Reuters* — **Nigeria: Bird flu virus spreads through north.** The H5N1 bird flu virus was confirmed in two more Nigerian states on Thursday, February 9, as authorities grappled to contain the disease with quarantine orders and culling. Nigeria reported Africa's first confirmed cases on Wednesday, February 8, of the highly pathogenic strain of avian influenza, which has forced the slaughter of more than 100 million birds in Asia and jumped to humans in Asia, Europe, and the Middle East. The bird flu outbreak was first reported at a poultry farm in northern Kaduna State, affecting tens of thousands of birds, but by Thursday authorities had reported new cases of fowls with H5N1 in neighboring Kano State and Plateau State. "The federal government is doing everything to contain the disease within the three centers that have been located," said a statement from Agriculture Ministry spokesperson Tope Ajakaiye. The U.S. has pledged $25 million to help Africa's most populous nation combat the disease, and is dispatching an expert team expected in the next four days from the U.S. Centers for Disease Control and Prevention, Ajakaiye added. Fowl have been dying in large numbers across northern Nigeria for the past four weeks and surveillance teams have been sent to scour northern Nigeria in search of suspect farms.
Source: http://www.alertnet.org/thenews/newsdesk/IRIN/cecf7efcba59a5d8c1890df41b41fba8.htm

28. *February 09, Kommersant (Russia)* — **Poultry farmers to be vaccinated.** Anton Katlinsky, head of one of the largest pharmaceutical producers in Russia, announced the development of a prototype of a new vaccine against bird flu. Plans are in place to vaccinate people who come into contact with domestic poultry with it if bird flu becomes epidemic. That disease is not contractible from person to person but only through contact with sick birds. Katlinsky said that the vaccination was made from virus samples obtained from the World Health Organization. Although the vaccine has not been subject to clinical trials yet, Katlinsky expressed readiness to produce it on an industrial scale. In January, the Russian Finance Ministry announced, following instructions from Russian President Vladimir Putin “not to let bird flu arise on the territory of Russia,” that $160 million would be allocated for epidemiological security in 2006. Katlinsky, who is a former deputy health minister, estimated that a minimum of 30 million doses of the vaccine will be needed in Russia. Other experts say that even more vaccine may be needed in Russia.
Source: http://www.kommersant.com/page.asp?idr=530&id=648089

29. *February 09, Agence France−Presse* — **China places 35 people under observation amid bird flu outbreak.** Health authorities in northern China have placed 35 people under observation after 15,000 fowl died of bird flu on the farm where they were working, state media said. The Xinhua news agency, citing government sources in Shanxi province, said the 35 workers had been confined to their homes in Yangquan city and were receiving twice−daily medical check−ups. Authorities have confirmed that the H5N1 strain of bird flu killed 15,000 head of poultry on their farm and said 187,745 more had been culled in the affected area to prevent the disease spreading. Bird flu has killed seven people in China. China has reported 34 H5N1 outbreaks among poultry since the beginning of last year, with most appearing since October.

Source: http://news.yahoo.com/s/afp/20060209/hl_afp/healthfluchina_060209172229;_ylt=AhslfuVucYuBLXCTLnzwr.KJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

30. *February 07, Oroville Mercury−Register (CA)* — **California unveils high−tech center.** California opened a statewide, public health disaster command center Tuesday, February 7. "This public health center will help save lives and reduce illness and injury," said state health services director Sandra Shewry. Her news conference provided a one−time public glimpse at the facility before a security lockdown. The center would be particularly critical in the event of bio−terrorism attacks, pandemic flu, West Nile Virus outbreaks, and other public health emergencies, such as floods that contaminate drinking water, Shewry said. The facility, jointly run by the state Department of Health Services and state Emergency Services Authority, would be in constant communication with the lead disaster facility, the state Office of Emergency Services command center in a Sacramento suburb. Those centers, in turn, would be in touch through video or audio conferencing with the U.S. Centers for Disease control and Prevention, the state Public Health Laboratory, and responding agencies. Experts from an array of agencies and fields, extending even to air quality and food safety, would man the 80 work stations on a 24−hour basis, each equipped with computers, telephones and other gear. The center features floor−to−ceiling, video−display monitors that can provide them links to 20 different visual sources.
Source: http://www.orovillemr.com/news/bayarea/ci_3485114

[Return to top]

Government Sector

31. *February 08, CNN* — **Senate nerve agent scare a false alarm.** A U.S. Senate office building was evacuated Wednesday evening, February 8, after a sensor detected the presence of a possible nerve agent, but it was later determined to be a false alarm, sources said. Capitol Police Chief Terrance Gainer said the building was "all clear" as footage from the scene showed the evacuees leaving the area where they had been gathered after the scare. Eight senators and more than 200 staffers were evacuated after alarms sounded at 7 p.m. EST in the attic of the Russell Senate Office Building, just north of the Capitol, Senate aides said Capitol Police spokesperson Sgt. Kimberly Schneider said she couldn't say whether it was powder, gas or liquid that was detected. It was more like "something in the air" in the building's attic, which takes up an entire floor of the 658,000−square−foot building, she said. She added that a cleaning solvent could have falsely set off the sensor in the attic, which is used primarily as storage space. Police said that no one had shown symptoms of exposure, leading one security expert to suspect a false alarm before it was even announced.
Source: http://www.cnn.com/2006/US/02/08/nerve.agent/index.html

[Return to top]

Emergency Services Sector

32.

February 08, Occupational Hazards — **White paper clarifies industrial hygienists' role in emergency response.** To help emergency planners, incident commanders and community leaders take full advantage of the experience, training and education of industrial hygiene professionals, the American Industrial Hygiene Association (AIHA) has developed a white paper that provides specific guidance on where and how these experts can fit into the Incident Command System, as specified by the National Incident Management System. Industrial hygienists' expertise can be a vital resource for government agencies, private response organizations and local emergency planning committees when preparing for or responding to emergency situations, according to AIHA. Qualified industrial hygienists can provide effective guidance on methods to identify, manage and ultimately control risks associated with natural disasters, hazardous material accidents and terrorist attacks, the professional organization believes. According to the white paper, industrial hygienists are qualified and able to perform a number of incident command functions, such as: Participating in pre−planning for a major incident; developing and implementing exposure assessment methods to identify and prioritize hazards during the incident response and consequence management phases of an operation; and interpreting data from sampling activities and direct−reading instrumentation appropriately.
AIHA white paper: http://www.aiha.org/1documents/GovernmentAffairs/EPRWhitePaper_Final.pdf
Source: http://www.occupationalhazards.com/articles/14690

33. *February 08, Tehachapi News (CA)* — **California organization is first in nation to conduct earthquake drill focused on water storage tank safety.** Last week, the Golden Hills Community Service District (CSD) held an earthquake response drill focused on water storage tank safety. The Golden Hills CSD is the first organization in the nation to address this important subject with actual drills. Ed Swenson, president of the organization that led the drill, is an expert on water tanks and earthquakes. His company, Los Osos Engineering, Inc., inspected water tanks all over Southern California after the 6.5−magnitude San Simeon earthquake in December 2003. The information garnered from that study was instrumental in developing this program, in which the ultimate objective is to teach post−seismic event forensics. In a major earthquake, the water inside a water tank sways with the ground, creating tremendous pressure inside the tank. The movement of the water can do severe damage to the tank. “After an earthquake, water tanks are the most vulnerable structures in a community,” Swenson said. After a major earthquake, damage to a water tank may be significant enough to warrant the closure and draining of the tank. This action can’t be taken lightly, however, because water is a valuable resource in fighting the fires that often follow earthquakes.
Source: http://www.tehachapinews.com/02082006/dri.html

34. *February 08, Spectrum (UT)* — **Utah county is one of 10 communities nation−wide to receive FEMA's community−specific training.** Emergency and government officials from throughout Washington County, UT, had a preview on Tuesday, February 7, of how a major mock disaster will stress their skills and training. As part of a weeklong integrated emergency management course taught by the Federal Emergency Management Agency (FEMA) at its Noble Training Center in Anniston, AL, the group is participating in three simulated exercises designed to test emergency response abilities. A simulation on Tuesday, February 7, featured a collision that resulted in a hazardous materials spill and a fire at an assisted living center that killed two residents. The simulation, like the major one the group faced Wednesday, February 8, focused on communication and cooperation rather than actual responses. Dean Cox,

Washington County Emergency Services coordinator, said the training has enforced the idea that Washington County can put together an area command comprising representatives from the county and various municipalities in preparation for disaster. Washington County is one of only 10 counties nation−wide to have a community−specific training like this from FEMA, Cox said.
Source: http://www.thespectrum.com/apps/pbcs.dll/article?AID=/20060208/NEWS01/602080313/1002

[Return to top]

Information Technology and Telecommunications Sector

35. *February 09, Reuters* — **Research in Motion unveils workaround plan.** Waterloo, Ontario−based Research In Motion (RIM) released on Thursday, February 9, details of a software workaround it has designed for its BlackBerry e−mail device as a backup plan if U.S. courts rule against the Canadian company in a patent dispute with U.S. company, NTP Inc. This workaround comes in advance of a Friday, February 24, hearing on a possible injunction shutting down most U.S. sales and service of BlackBerry.
Source: http://today.reuters.com/News/newsArticle.aspx?type=businessNews&storyID=2006−02−09T120440Z_01_N09386995_RTRUKOC_0_US−RESEARCHINMOTION.xml

36. *February 09, Associated Press* — **Europe urged to improve Web security.** Europe must work harder to make the Internet more secure as the nature of online threats becomes increasingly criminal across the 25−nation bloc, a senior EU official warned Thursday, February 9. "We are still far from achieving the goal of secure and reliable networks that protect confidential and reliable information," said Viviane Reding, the EU's media commissioner, at a conference on trust in the Internet. Almost 80 percent of EU citizens are concerned about Internet security and half do not engage in electronic commerce because they worry about having their personal financial data stolen on the Web, she said. Speaking via video link from Brussels, Reding stressed the importance of international cooperation in promoting user trust in the Web and said she would soon announce a "strategy for enhanced security."
Source: http://news.yahoo.com/s/ap/20060209/ap_on_hi_te/eu_internet_security;_ylt=AqJsTFxWQORMKXpiJ5yFMsAjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

37. *February 08, eWeek* — **Effects of domain hijacking can linger.** Malicious hackers who are able to hijack an organization's Web domain may be able to steal traffic from the legitimate Website long after the domain has been restored to its owner, according to a recent report. Design flaws in the way Web browsers and proxy servers store data about Websites allow malicious hackers to continue directing Web surfers to malicious Webpages for days or even months after the initial domain hijacking. The persistent attack could lead to information or identity theft, according to Amit Klein, a Web application security researcher with the Web Application Security Consortium. The problem, which Klein termed "domain contamination" exists because of features in Web proxy servers, which store versions of Webpages, and Web "clients," or browsers, including Microsoft's Internet Explorer, the Mozilla Foundation's Firefox and the Opera browser. Proxy servers and browsers both establish trust relationships with Web

servers that are identified as the authoritative host for a Webpage in the DNS (domain name system), Klein said. "Once a client believes it is communicating with the legitimate server for some domain, there's an implicit trust that's placed in that server that is not revoked," said Klein.
Report: Domain Contamination: http://www.webappsec.org/projects/articles/020606.shtml
Source: http://www.eweek.com/article2/0,1895,1923546,00.asp

38. *February 08, IDG News Service* — **Bush signs digital TV transition bill.** U.S. President George Bush on Wednesday, February 8, signed into law legislation setting February 17, 2009, as the date U.S. broadcasters must end transmitting analog television signals and move to all−digital broadcasts. The move from the upper 700MHz spectrum band will free up 60MHz for auction to mobile wireless carriers and 24MHz for emergency response agencies. The upper 700MHz band will allow wireless signals to travel four to five times as far as existing mobile phone signals, advocates of the digital television (DTV) deadline said. That makes the spectrum valuable for mobile broadband providers and for police and fire departments that want to communicate better with regional counterparts. Under current law, broadcasters are required to give up their analog spectrum by the end of 2006, but only in television markets where 85 percent of homes can receive digital signals.
Source: http://www.infoworld.com/article/06/02/08/75193_HNbushbroadb and_1.html

39. *February 08, Associated Press* — **Websites hawking phone records shut down.** Following a wave of negative publicity and pressure from the government, several Websites that peddled people's private phone records are calling it quits. "We are no longer accepting new orders" was the announcement posted Wednesday, February 8, on two such sites, locatecell.com and celltolls.com. The Federal Trade Commission (FTC) this week conducted a sweep of 40 sites known to have been selling private phone records. According to the FTC's Lydia Parnes, more than 20 sites have recently shut down or stopped advertising for new business. The agency has sent letters to about 20 other sites, warning them that they may be violating the law and should review their business practices, said Parnes, director of the FTC's Bureau of Consumer Protection. While some sites appear to be closing up shop, others have seen a boom in business with the recent media attention, said Marc Rotenberg, executive director of the Electronic Privacy Information Center. Rotenberg urged lawmakers to ban a practice known as "pretexting," in which data brokers or others call a phone company, impersonate a customer and then persuade the company to release the calling records.
Source: http://www.nytimes.com/aponline/technology/AP−Phone−Records.html?_r=1&oref=slogin

40. *February 06, Computer World* — **Machine−learning techniques to create self−improving software are hitting the mainstream.** Attempts to create self−improving software date to the 1960s. But "machine learning," as it's often called, has remained mostly the province of academic researchers, with only a few niche applications in the commercial world, such as speech recognition and credit card fraud detection. Now, researchers say, better algorithms, more powerful computers and a few clever tricks will move it further into the mainstream. Computer scientist Tom Mitchell, director of the Center for Automated Learning and Discovery at Carnegie Mellon University, says machine learning is useful for the kinds of tasks that humans do easily, but that they have trouble explaining explicitly in software rules. In machine−learning applications, software is "trained" on test cases devised and labeled by

humans, scored so it knows what it got right and wrong, and then sent out to solve real−world cases. Mitchell is testing the concept of having two classes of learning algorithms in essence train each other, so that together they can do better than either would alone. Mitchell's experiments have shown that such "co−training" can reduce errors by more than a factor of two. The breakthrough, he says, is software that learns from training cases labeled not by humans, but by other software.
Source: http://www.computerworld.com/developmenttopics/development/story/0,10801,108320,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of several vulnerabilities in Mozilla. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary JavaScript commands with elevated privileges or cause a denial of service condition on a vulnerable system.

For more information please review US−CERT Vulnerability Note:

VU#592425
Mozilla based browsers fail to validate user input to the attribute name in "XULDocument.persist" at URL:

http://www.kb.cert.org/vuls/id/592425

US−CERT urges users and administrators to implement the following recommendations.

Review updates to:

Firefox 1.5.0.1: http://www.mozilla.com/firefox/

SeaMonkey 1.0: http://www.mozilla.org/projects/seamonkey/

Disable JavaScript in Thunderbird and Mozilla Suite.

Current Port Attacks

Top 10 Target Ports	4556 (−−−), 1026 (win−rpc), 6881 (bittorrent), 15266 (−−−), 25 (smtp), 445 (microsoft−ds), 3800 (−−−), 135 (epmap), 80 (www), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer